perimeter 81

CYBERSEC SOLUTIONS

ZTNA vs On-Premises Firewall VPN

for the Remote Workspace

Securing Today's Remote Workspaces

As hybrid work becomes the new normal, companies are looking for innovative ways to provide secure remote access to employees in and out of the office.

Hardware firewall VPNs of the past often don't answer today's need for secure remote access, leaving organizations vulnerable to security breaches and increasing the chances of cyber attacks across their networks.

That's because they give users within the organization access to the entire internal network in order to access company resources. With legacy firewalls, complex configuration makes it difficult to restrict users and devices from accessing specific applications. Without granular access controls, the security risk is increased due to an increased attack surface.

From segmented user access to seamless scalability, Zero Trust Network Access (ZTNA) provides IT admins with an all-encompassing solution to secure their resources, on-prem and in the cloud.

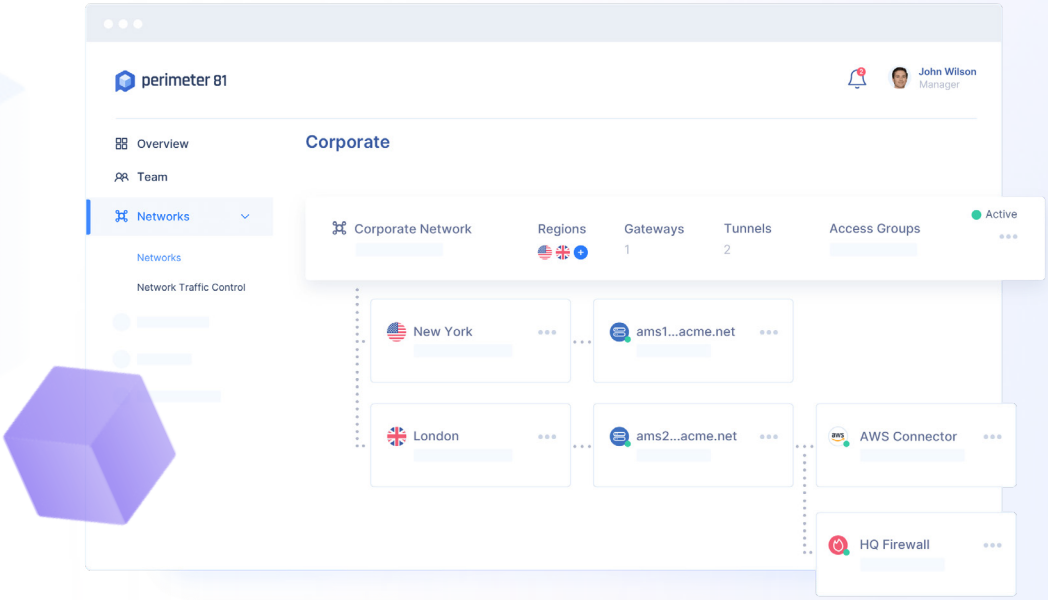
Enterprise Level Network Security with Zero Trust

The traditional approach of physical firewalls grants implicit trust to any device, user, and application within a given network that enters via the VPN tunnel. This means that compromised VPN credentials or exploitation of a VPN vulnerability can lead to malicious “authenticated” access by attackers who can move laterally through the network.

Zero Trust Network Access (ZTNA) grants access to corporate resources based on the principle of zero trust, or least privilege. Users are granted access to what they need and where they need it to carry out their role, so only identified employees can access the corporate network.

ZTNA solutions provide a flexible cloud-based platform, device and application configurability as well as accessibility, increased security, privacy and user-access control granularity and analytics. Moreover, they do it from a single management platform that gives IT a 360-degree view of access and security.

By reducing the attack surface of exposed hosts, ZTNA solutions help reduce data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking and malicious insiders.



What is ZTNA?

Zero Trust Network Access is a security model in which access to on-prem and cloud resources is carefully segmented and monitored, allowing only trusted employees to access company assets. By implementing the Zero Trust, “never trust, always verify” approach, organizations can significantly decrease the attack surface and protect their valuable resources.

ZTNA is a combination of security tools that identify, authenticate and verify each company user, making sure they have the proper identification and credentials to access company addresses and services. ZTNA includes features such as Firewall as a Service, two-factor authentication and network segmentation to fully control user activity in and out of the network.

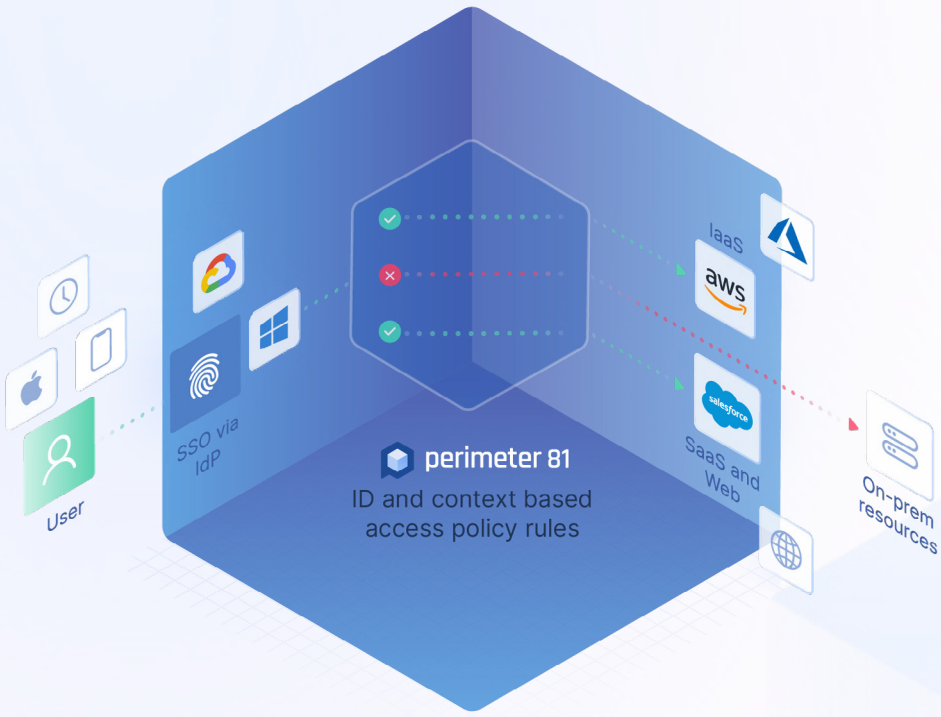
- **ZTNA starts by identifying users**, via Identity Provider integration and Multi-Factor Authentication, and the context behind their requests for access through the unified ZTNA solution.
- **Access is either blocked or permitted** by the ZTNA solution based on identity, context, and ZTNA rules that determine what identity and context are required to access each resource.
- **When combined with virtual network segmentation** using Firewall as a Service (FWaaS) implemented in the ZTNA platform, a hacker with stolen credentials will have their access limited to only specific areas and will not be able to fully traverse the network. This approach significantly reduces the level of exposure and can prevent detrimental damage to a company’s data.

It’s no surprise that ZTNA guarantees the best network solution for organizations worldwide. In order to limit the attack surface and decrease the chances of online threats, more IT managers are dropping hardware firewalls in exchange for a broader and safer ZTNA solution.

Comparing ZTNA vs On-Prem Firewall VPN

	Zero Trust Network Access	On-Premises Firewall VPN
Unified Management	Networks and users are easily managed from one single platform	Each firewall is individually managed across multiple offices with complex interfaces
Network Performance	Faster connection, better network performance across +50 data centers	Fewer data centers on-prem, non-optimal traffic routing may cause users to experience low performance
User Identification and Authentication	Privatized user access with identification and multi-factor authentication	User identities managed across multiple firewalls. Only some IDPs are supported
Cost Reduction	Cloud based ZTNA reduces configuration complexity and onboarding time. Cloud security service eliminates need for storage and maintenance	Hardware requires manual installation, configuration, physical storage space, cooling, and ongoing maintenance. Requires trained personnel to instal and upgrade
Device Posture Check	Devices are checked for security posture before accessing resources	No devices undergo a posture check
Zero Trust Application Access	Trusted clientless access to apps without exposing users to the whole network	No segmented application access

User Onboarding	Adding users and expanding networks can be done in minutes	Scaling is often a complicated and manual process requiring installations
Network Visibility	Single interface for entire network visibility	Network visibility is often a manual process
Compliance	Meets security compliance requirements	Meets security compliance requirements
Traffic Encryptions	All traffic is encrypted end-to-end	All traffic is encrypted end-to-end
Micro-Segmentation	Segmented user access across network resources	Segmenting user access can be complicated and performance may be hindered
Added Protection	Features such as SWG must be integrated into ZTNA as an additional process	Firewall capabilities extend to anti-malware and intrusion prevention systems



The 5 Limitations of a Firewall VPN for Accessing Remote Resources

1

Difficult to Install and Manage

A physical firewall requires manual insulation, configuration and management while ZTNA makes it easy to change policies in just a few clicks.

2

Reduced Network Performance for the Remote Workspace

Hardware firewalls are limited to fewer data centers so employee connectivity is often slower and less optimal. ZTNA connects remote workers to over 50 data centers, ensuring smooth network performance.

3

Limited Security

Physical firewalls don't check for device posture security. With ZTNA, device posture check is implemented along with Identity Provider integrations and Multi-Factor Authentication, creating a protective barrier from potential attacks.

4

Harder to Scale

It's often complicated to add new networks and users with a firewall. A unified cloud platform, lets you make these changes easily over a single interface with little room for error.

5

Limited User Segmentation

Hardware firewall VPNs can't grant clientless access to third-party contractors. ZTNA is able to segment granular access to specific apps, keeping users from exposure to the network at large.

ZTNA for a Safer Hybrid Workspace

By controlling all aspects of network security with a Zero Trust solution, IT managers can significantly reduce the risks of online threats - in ways a firewall simply can't.

Reliable Network Performance

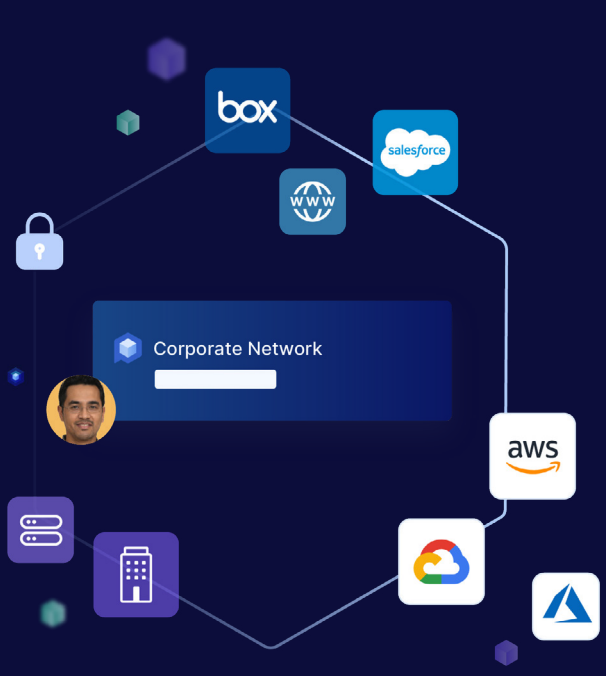
With over 50 global PoPs, Perimeter 81's ZTNA solution allows users to connect to the nearest data center with minimal latency and optimized network performance.

Unified Management

Being a cloud platform, ZTNA allows IT admins to manage all their network activities in one place.

Enhanced Security

ZTNA ensures advanced network security with features such as Device Posture Check, Secure Web Gateway and cloud identity providers.



More and more security professionals are replacing physical firewalls with ZTNA to better protect their organization's most valuable resources both on-premise and in the cloud. Zero Trust ensures relevant least-privilege and secure access to corporate resources, limiting the attack surface and decreasing the chances of online attacks.

Perimeter 81's ZTNA Solution

Perimeter 81 offers a powerful cloud-based ZTNA solution built into its Security Service Edge (SSE) platform.

- Perimeter 81's ZTNA solution ensures that users access cloud resources via encrypted tunnels directly from the Perimeter 81 network, to lock down network resources and application access using Zero Trust policies.
- The Perimeter 81 network is global with over 50 PoPs located across the globe. ZTNA ensures that users only have access to the resources they need.
- DNS filtering adds another layer of protection to ensure users cannot access risky websites. The Perimeter 81 solution secures access to any network resource: on-prem data centers, public cloud (AWS, Azure, GCP), or the private cloud via an IPsec or Wireguard tunnel.
- Perimeter 81 supports all ports and protocols, including non-web applications like VoIP. Each Perimeter 81 gateway offers 1 Gb/s of bandwidth.

The Perimeter 81 platform is the right solution in a world where accelerating complexity is the single greatest threat to effective network security.

Get the most out of Zero Trust

Instant Deployment

In just a few clicks, Perimeter 81 allows you to purchase, provision, and enable secure zero-trust access on-prem, in the cloud, and anywhere in between. Quickly scalable microservice architecture and transparent pricing allow you to easily grow, backed by our 24/7 Customer Success engineers.

Integrated Security

Avoid the complexity of using dozens of cybersecurity solutions with a single well-designed platform that makes it easy to configure your network, implement security policies, detect active attacks, and defend against data breaches.

Unified Management

Effortlessly manage and onboard network users, instantly deploy secure cloud gateways, create multi-regional networks, and install cross-platform applications across all endpoints within a single dashboard.

Full Visibility

Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity with a unified view of your network security.

About Perimeter 81

Perimeter 81 radically simplifies network security with an award-winning Security Service Edge (SSE) platform. As a holistic, cloud-based solution, Perimeter 81 allows organizations of all industries and sizes to easily support the decentralized, hybrid workplace while avoiding the cyber complexity that hurts IT's ability to defend corporate cloud and on-prem networks. Backed by Tier 1 Investors such as Insight Partners, Toba Capital, and others, Perimeter 81 is headquartered in Tel Aviv, the heart of the startup nation, and has US offices in New York and Los Angeles. Our 2,500 customers range from SMBs to Fortune 500s across a wide range of industries, and our partners are among the world's leading integrators, managed service providers, and channel resellers.

Contact Cybersec Solutions

Tel: 01494 936696 | Email: info@cybersec.solutions | Web: www.cybersec.solutions